(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 391 083 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
30.11.2011 Bulletin 2011/48

(21) Application number: **09838652.7**

(22) Date of filing: **15.09.2009**

(51) Int Cl.:
H04L 29/06 *(2006.01)*

(86) International application number:
PCT/CN2009/073942

(87) International publication number:
WO 2010/083685 (29.07.2010 Gazette 2010/30)

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(30) Priority: **22.01.2009 CN 200910105248**

(71) Applicant: **ZTE Corporation**
Shenzhen, Guangdong 518057 (CN)

(72) Inventors:
- **CUI, Zhenfeng**
  Shenzhen
  Guangdong 518057 (CN)
- **BIAN, Zhijun**
  Shenzhen
  Guangdong 518057 (CN)
- **CHEN, Xi**
  Shenzhen
  Guangdong 518057 (CN)

(74) Representative: **Sander Jakobsson, Sofia Ellinor**
Awapatent AB
Junkersgatan 1
582 35 Linköping (SE)

(54) METHOD FOR REALIZING AUTHENTICATION CENTER AND AUTHENTICATION SYSTEM

(57) A method for realizing an authentication center (AC) and an authentication system are disclosed. The method comprises: a UE sends an authentication request to an AC and applies for temporary authentication information, the AC assigns a first authentication random code to the UE, then the UE calculates a first response code and sends it to the AC, the AC assigns the temporary authentication information to the UE after authentication and authorization; the UE sends a login request to the application system (AS) which assigns a second authentication random code to the UE, and the UE uses it and the temporary authentication information to calculate a second response code, and sends this code to the AS; the AS sends the second response code to the AC for authentication and authorization; the AC returns the authentication result to the AS which in turn returns the authentication result to the UE. Since the temporary authentication information is featured with uniqueness and timeliness, it has enough security, thus the present invention can be widely applied in the field of authentication.

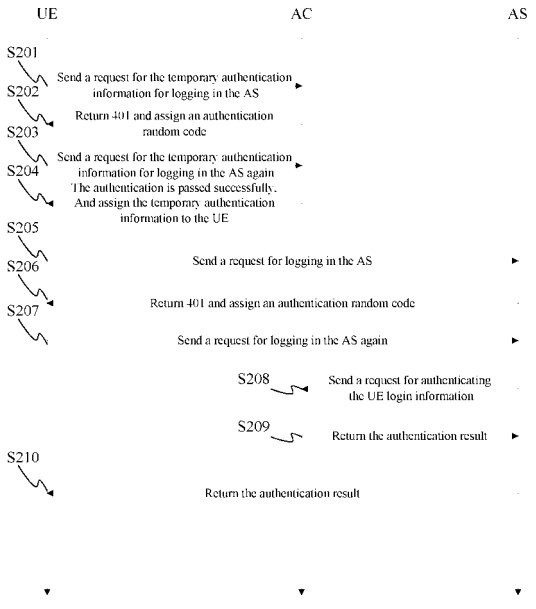

FIG. 2

EP 2 391 083 A1

Description

Technical Field

[0001] The present invention belongs to the field of user ID authentication, and more especially, to a method for realizing a user ID authentication center in an multi-application system with relatively high security requirements and an authentication system thereof.

Background of the Related Art

[0002] With the development of industry services, the number of industry service application systems increases rapidly. To date, the user ID authentication is implemented by the application system of each service in most cases, therefore, in order to access different application systems, the user has to input his/her user credence to different application systems respectively. In the case that the number of application systems increases rapidly and marketization develops very quickly, the disadvantage of this mode is more and more evident and becomes especially prominent particularly under the condition that the application system increases exponentially. Although the existing system has implemented unique authentication for the user ID, it is mainly by sending the response code and random code acquired by calculating the user token to the authentication center to perform authentication and authorization. If this information is intercepted, the trust of the authentication center can be gained unlimited by cheating, which brings severe threats to information security. Therefore, it is necessary to provide a method for realizing the authentication of the information security.

Content of the Invention

[0003] The purpose of the present invention is to provide a method for realizing an authentication center with relatively high security performance and an authentication system to overcome the shortcomings in the prior art, the method provided in the present invention can not only uniquely authenticate the user ID, but also have enough security.

[0004] In order to solve the above technical problem, the present invention is implemented with the following technical scheme:

A method for realizing an authentication center, and the method comprises the following steps of:

A. a user equipment (UE) sending an authentication request to an authentication center (AC) and applying for temporary authentication information for logging in the application system, the AC assigning a first authentication random code to the UE, and the UE calculating a first response code according to this first authentication random code and sending the first response code to the AC, after the authenticating and authorizing the UE, the AC assigning the temporary authentication information to the UE;

B. the UE sending a login request to the application system, and the application system assigning a second authentication random code to the UE, the UE calculating a second response code according to the second authentication random code and said temporary authentication information, and sending the second response code to the application system;

C. the application system sending the second response code to the authentication center, and the authentication center performing authentication and authorization; and

D. the authentication center returning the authentication result to the application system, and the application system returns the authentication result to the UE.

[0005] In the above method, said first and said second authentication codes can exist in the form of MD5 (message-digest algorithm 5).

[0006] In the above method, MD5 and SHA1 (Secure Hash Algorithm) combined algorithm can be used in the step of calculating the first and the second response codes.

[0007] In the above method, said temporary authentication information might comprise the UE account, the application system ID and a temporary token.

[0008] In the above method, said temporary authentication information might be featured with uniqueness and timeliness, and it is valid for about one minute.

[0009] In the above step A, the authentication center might directly use a symmetrical secure encryption algorithm, secure socket layer (SSL), or transport layer security (TLS) to transmit the temporary authentication information which is assigned to the UE.

[0010] Said symmetrical encryption algorithm that can be directly used might be data encryption standard (DES), triple DES (3DES) or advanced encryption standard (AES).

[0011] In said step C, if the authentication is passed successfully, the authentication center might clear said temporary authentication information.

[0012] In addition, the present invention also provides an authentication center, a user equipment, an application system and an authentication system to solve the above technical problem.

[0013] The authentication center, configured to:

receive an authentication request as well as an application for temporary authentication information for logging in the application system from the UE, assign

a first authentication random code to said UE, receive a first response code calculated according to said first authentication random code and sent by said UE, and assign said temporary authentication information to said UE after the authentication and authorization;

receive a second response code from said application system and perform authentication and authorization, wherein, said second response code is calculated out by said UE according to the second authentication random code assigned by the application system and the temporary authentication information after said UE sends a login request to the application system; and

return the authentication result to said application system, so that said application system can return the authentication result to said UE.

[0014] In said authentication center, said temporary authentication information might comprise the UE account, the application system ID and a temporary token.

[0015] In said authentication center, said temporary authentication information is featured with uniqueness and timeliness.

[0016] Said authentication center is also configured to receive the second response code sent by said application system, and clear said temporary authentication information if the authentication is passed successfully when performing the authentication and authorization.

[0017] The user equipment, configured to:

send an authentication request to the authentication center and apply for temporary authentication information for logging in the application system, receive the first authentication random code assigned by said authentication center, calculate the first response code according to said first authentication random code and send said first response code to said authentication center, receive said temporary authentication information assigned by the authentication center after the authentication and authorization;

send a login request to said application system, receive the second authentication random code assigned by the application system, calculate said second response code according to said second authentication random code and said temporary authentication information, and send said second response code to said application system; and

receive the authentication result returned from said application system, wherein said authentication result is returned by said authentication center to the application system after said application system sends the second response code to the authentication center and said authentication center performs the authentication and authorization.

[0018] The application system, which is configured to:

respond the login request sent from the UE, assign the second authentication random code to said UE, receive the second response code sent from said UE, wherein said second response code is calculated out by said UE using said second authentication random code and the temporary authentication information, wherein said temporary authentication information is assigned by said authentication center after authentication and authorization based on the first response code calculated out by said UE according to the first authentication random code assigned by said authentication center and sent by the user equipment after said UE sends an authentication request to the authentication center and applies for temporary authentication information for logging in the application system;

sending said second response code to said authentication center, and after authentication and authorization are performed in said authentication center, receive the authentication result returned from said authentication center, and send the authentication result to said UE.

[0019] An authentication system, comprising the above authentication center, the UE and the application system.

[0020] Using the method for implementing an authentication center in accordance of the present invention has the following benefit effects:

Since the temporary token is generated according to a specific application system and it has timeliness, it can guarantee the security of the user temporary authentication information, furthermore, the method for implementing the authentication center has enough security.

Brief Description of Drawings

[0021]

FIG. 1 is a networking schematic diagram of the authentication system in accordance with the present invention; and

FIG. 2 is a flow chart of signaling of each network element in the authentication system of the present invention.

Preferred Embodiments of the Present Invention

[0022] In order to understand the present invention

better, the present invention will be illustrated in further detail in combination with the accompanying figures and embodiments.

[0023] Refer to FIG. 1, the authentication system comprises client UE 4, application server AS 3 (corresponding to the application system) and authentication center AC1 which are connected together via access gateway 2. FIG. 1 takes the UE as an example, and UE 4 uses the services offered by AS3; AC1 is used to authenticate and authorize UE4.

[0024] Refer to FIG. 2 which is a flow chart of signaling of each network element in the authentication system of the present invention, it takes the hypertext transfer protocol (HTTP) as the interface between the UE and the AC, and takes the simple object access protocol (SOAP) between the AS and the AC as an example to describe the flow chart of the implementation of the authentication center, and the implementation comprises the following steps:

Step 201: Before using the AS service officially, the UE sends an authentication request to the AC, meanwhile it applies for temporary authentication information for logging in the AS;

Step 202: the AC returns 401 (request for authentication) and assigns an authentication random code;

Step 203: the UE uses the authentication random code assigned by the AC to calculate a response code, and sends the response code to the AC;

Step 204: the AC authenticates and authorizes the UE, and assigns the UE the temporary authentication information for logging in the AS, where the temporary authentication information comprises the UE account, the application system ID (the AS ID) and a temporary token. Wherein, the AS ID is the identifier assigned to the AS by the AC, and it is a globally unique identifier (GUID); in order to securely send the temporary authentication information to the UE, the following secure modes can be applied:

1) directly use a symmetrical encryption algorithm

The encryption algorithm comprises DES, 3DES, AES, and so on, wherein, the DES has high speed and is suitable to scenarios of encrypting a lot of data and systems with relatively low security requirements; the 3DES is based on the DES, uses three different tokens to encrypt a block of data for three times, has higher security, and is used to the systems with relatively high security requirement; the AES is the next generation encryption algorithm standard and has high speed, high security level, and is suitable to encrypt digital information in the fields of finance, telecommunication and government;

2) SSL/TLS

Step 205: the UE sends a login request to the AS;

Step 206: the AS returns 401 (i.e. requests for authentication), and assigns an authentication random code; considering the token security, the authentication random codes of the AC and AS can be saved in the form of MD5, and the MD5 and SHA1 combined encryption algorithm can be used to calculate the response code, which is more secure;

Step 207: the UE uses the authentication random code assigned by the AS and the temporary authentication information assigned by the AC to calculate a response code and sends the response code to the AS;

Step 208: the AS sends the response code of the UE to the AC transparently;

Step 209: the AC performs the authentication and authorization according to the application identifier of the AS and the response code transparently transmitted by the AS, and returns the authentication result to the AS, if the authentication is passed successfully, the AC clears the temporary authentication information;

Step 210: the AS returns the authentication result to the UE.

[0025] In the above process, the temporary authentication information is uniquely assigned by the AC according to the AS which the UE accesses, and it is unique and has timeliness (the valid period is about one minute), and can be used only once, which largely increases the security of the authentication.

[0026] The above description is only preferred embodiments rather than the restriction of the scope of the present invention, and it should be pointed out that, for those skilled in the field, any modifications, equivalent alternatives and improvement made within the spirit and essence of the present invention should belong to the scope of the claims of the present invention.

Industrial Applicability

[0027] In the present invention, since the temporary token is generated according to a specific application system, and the token has timeliness, it can guarantee the security of the user temporary authentication information, so that the method for implementing the authen-

tication center has enough security.

Claims

1. A method for realizing an authentication center, and the method comprising:

   A. a user equipment sending an authentication request to an authentication center and applying for temporary authentication information for logging in an application system, the authentication center assigning a first authentication random code to the user equipment, and the user equipment calculating a first response code according to the first authentication random code and sending the first response code to the authentication center, after authenticating and authorizing the user equipment, the authentication center assigning the temporary authentication information to the user equipment;
   B. the user equipment sending a login request to the application system, and the application system assigning a second authentication random code to the user equipment, the user equipment calculating a second response code according to the second authentication random code and said temporary authentication information, and sending the second response code to the application system;
   C. the application system sending the second response code to the authentication center, and the authentication center performing authentication and authorization; and
   D. the authentication center returning an authentication result to the application system, and the application system returning the authentication result to the user equipment.

2. The method of claim 1, wherein, said first and said second authentication random codes exist in a form of message-digest algorithm MD5.

3. The method of claim 1 or 2, wherein, message-digest algorithm MD5 and secure hash algorithm SHA1 combined algorithm are used in the step of calculating the first and the second response codes.

4. The method of claim 3, wherein, said temporary authentication information comprises a user equipment account, an application system identifier and a temporary token.

5. The method of claim 4, wherein, said temporary authentication information is featured with uniqueness and timeliness.

6. The method of claim 4, wherein, in the step A, the step of the authentication center assigning the temporary authentication information to the user equipment comprises: directly using a symmetrical secure encryption algorithm or a secure socket layer (SSL) / transport layer security (TLS) to transmit the temporary authentication information.

7. The method of claim 6, wherein, said symmetrical encryption algorithm that is directly used is data encryption standard (DES), triple data encryption standard (3DES) or advanced encryption standard (AES).

8. The method of claim 1, wherein in the step of the authentication center performing authentication and authorization in said step C, the authentication center clear said temporary authentication information if the authentication is passed successfully.

9. An authentication center, configured to:

   receive an authentication request as well as an application for temporary authentication information for logging in an application system from a user equipment, assign a first authentication random code to said user equipment, receive a first response code calculated according to said first authentication random code and sent by said user equipment, and assign said temporary authentication information to said user equipment after authentication and authorization;
   receive a second response code from said application system and perform authentication and authorization, wherein, said second response code is calculated out by said user equipment according to the second authentication random code assigned by the application system and the temporary authentication information after said user equipment sends a login request to the application system; and
   return an authentication result to said application system, so that said application system can return the authentication result to said user equipment.

10. The authentication center of claim 9, wherein, said temporary authentication information comprise a user equipment account, an application system identifier and a temporary token.

11. The authentication center of claim 9, wherein, said temporary authentication information is featured with uniqueness and timeliness.

12. The authentication center of claim 9, wherein, said authentication center is also configured to receive a second response code sent by said application system, and clear said temporary authentication infor-

mation if the authentication is passed successfully when performing authentication and authorization.

13. A user equipment, configured to:

send an authentication request to an authentication center and apply for temporary authentication information for logging in an application system, receive a first authentication random code assigned by said authentication center, calculate a first response code according to said first authentication random code and send said first response code to said authentication center, receive said temporary authentication information assigned by the authentication center after authentication and authorization;
send a login request to said application system, receive a second authentication random code assigned by the application system, calculate said second response code according to said second authentication random code and said temporary authentication information, and send said second response code to said application system; and
receive an authentication result returned from said application system, wherein said authentication result is returned by said authentication center to the application system after said application system sends the second response code to the authentication center and said authentication center performs authentication and authorization.

14. An application system, configured to:

respond a login request sent from a user equipment, assign a second authentication random code to said user equipment, receive a second response code sent from said user equipment, wherein said second response code is calculated out by said user equipment using said second authentication random code and temporary authentication information, wherein said temporary authentication information is assigned by said authentication center after authentication and authorization based on a first response code calculated out by said user equipment according to a first authentication random code assigned by said authentication center and sent by the user equipment after said user equipment sends an authentication request to the authentication center and applies for temporary authentication information for logging in an application system; send said second response code to said authentication center, and after authentication and authorization are performed in said authentication center, receive an authentication result returned from said authentication center, and send the authentication result to said user equipment.

15. An authentication system, comprising the authentication center of any claim from claim 9 to claim 12, the user equipment of claim 13 and the application system of claim 14.

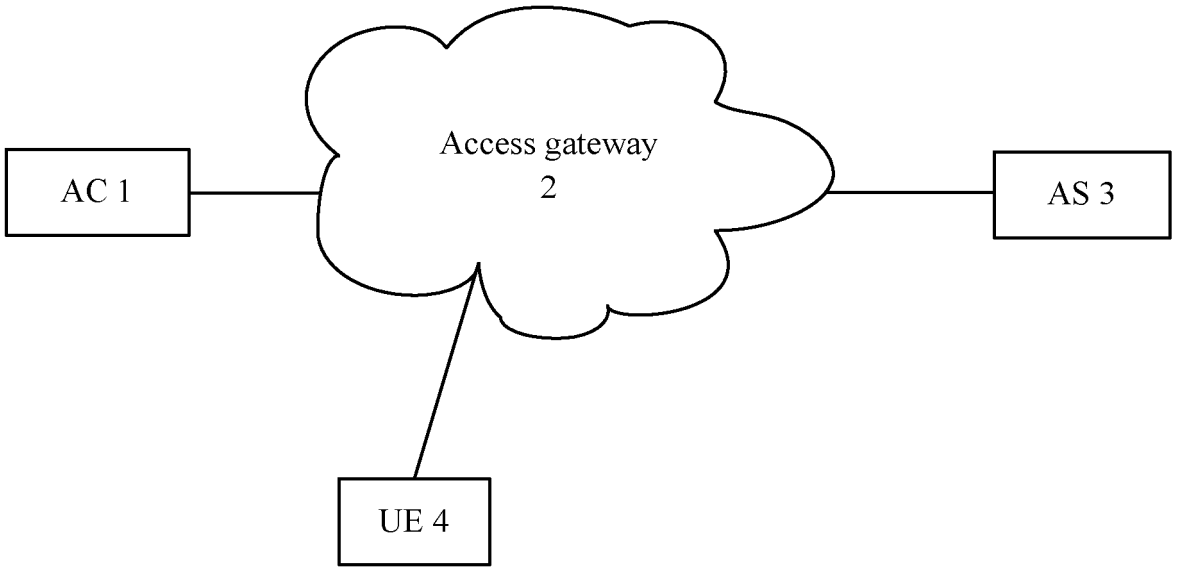

FIG. 1

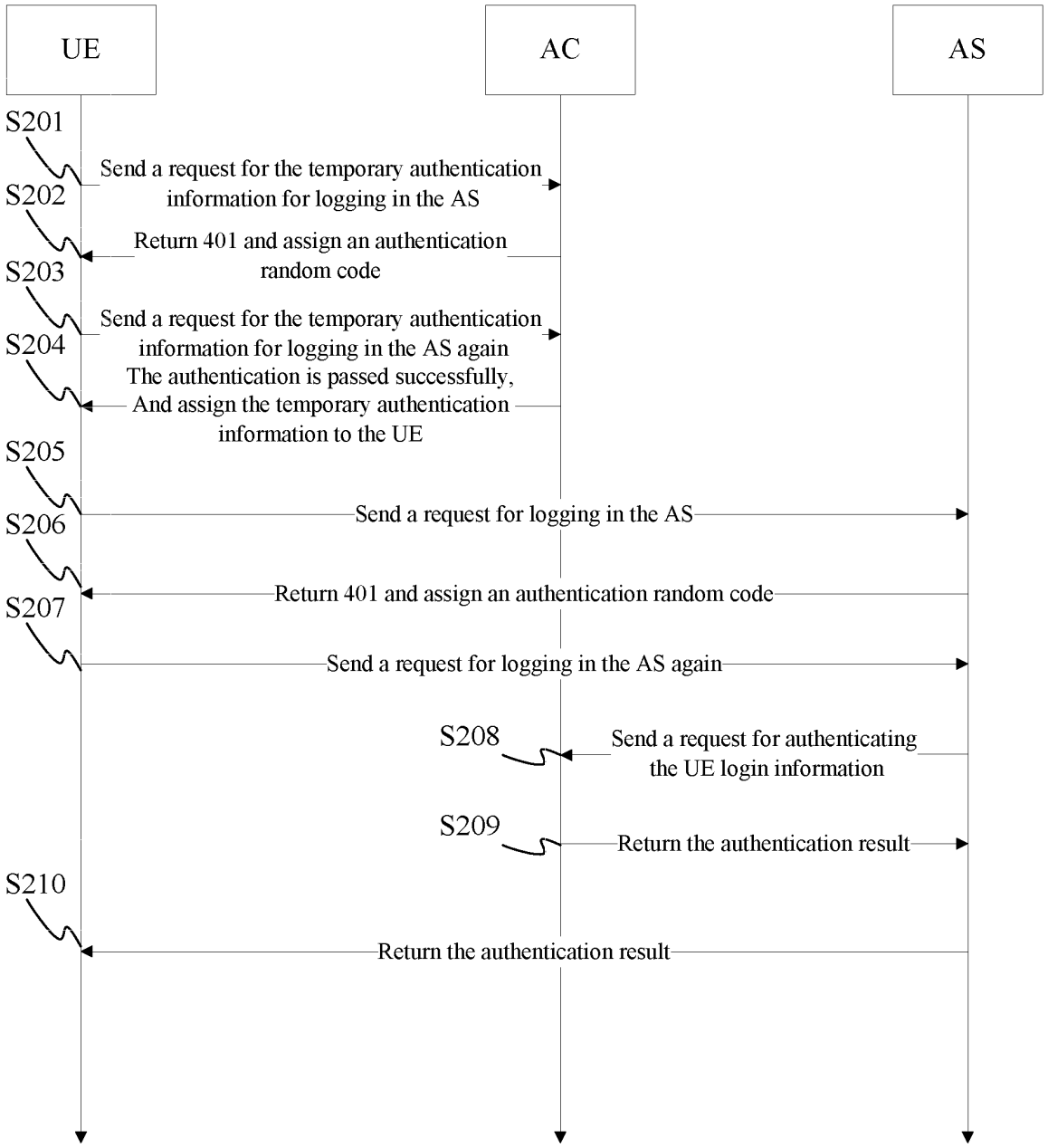
UE
AC
AS
S201
Send a request for the temporary authentication information for logging in the AS
S202
Return 401 and assign an authentication random code
S203
Send a request for the temporary authentication information for logging in the AS again
S204
The authentication is passed successfully, And assign the temporary authentication information to the UE
S205
Send a request for logging in the AS
S206
Return 401 and assign an authentication random code
S207
Send a request for logging in the AS again
S208
Send a request for authenticating the UE login information
S209
Return the authentication result
S210
Return the authentication result

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/073942

A. CLASSIFICATION OF SUBJECT MATTER

H04L29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L; H04Q; H04N; G03G; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI,EPODOC,PAJ:temporary,authenticat+,authorizat+,random,code,customer,subscriber,terminal,application,access+, log w in
CNPAT,CNKI:

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1529531A(ZHONGXING COMMUNICATION CO LTD) 15 Sep. 2004(15.09.2004) the whole document	1-15
A	CN101188606A(ZHONGXING COMMUNICATION CO LTD) 28 May 2008(28.05.2008) the whole document	1-15
A	CN1747382A(XU Wenxiang) 15 Mar. 2006(15.03.2006) the whole document	1-15
A	CN1983071A(RICOH KK) 20 June 2007(20.06.2007) the whole document	1-15
PX	CN101483525A(ZHONGXING COMMUNICATION CO LTD) 15 July 2009(15.07.2009) the whole document	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 Nov. 2009(10.11.2009)	**17 Dec. 2009 (17.12.2009)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer XIONG Yushan Telephone No. (86-10)62411467

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/073942

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1529531A	15.09.2004	none	
CN101188606A	28.05.2008	none	
CN1747382A	15.03.2006	none	
CN1983071A	20.06.2007	CN100474276C	01.04.2009
		JP2007172588A	05.07.2007
		US2007118734A1	24.05.2007
CN101483525A	15.07.2009	none	

Form PCT/ISA /210 (patent family annex) (July 2009)